UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993

24956 7590 05/21/2010

MATTINGLY & MALUR, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
05/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/940,982	ENDO ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20100510*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1. A response was received on 09 March 2010. By this response, Claims 1 and 28 have been amended. Claim 3 has been canceled. No new claims have been added. Claims 1 and 28 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 09 March 2010 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1 and 28 under 35 U.S.C. 103(a) as unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518, Applicant argues that the admitted prior art does not disclose "a selector for selecting disturbance data" or "disturbance data processing means performing predetermined processing on the selected disturbance data to generate processed disturbance data" as asserted in the previous Office action (see pages 6-7 of the present response, citing page 10 of the previous Office action and page 21, lines 1-12 of the present specification). However, the admitted prior art explicitly discloses "using a result of processing the data for disturbance" (page 21, lines 1-12, as quoted by Applicant) which is seen as support for the "disturbance data processing means" as claimed, as stated in the previous Office action. The admitted prior art also at least inherently discloses the

selection of disturbance data; if some piece of disturbance data is used, then it must have been selected for use.

Applicant further argues that a table of candidates of disturbance data is neither taught nor suggested by the admitted prior art or Jaffe (page 7 of the present response, citing page 10 of the previous Office action, and Jaffe, column 16, line 61-column 16, line 14). More specifically, Applicant asserts that the cited portion of Jaffe "only peripherally references look-up tables" but that this does not suggest a table of candidates of disturbance data (see pages 7-8 of the present response). However, the previous Office action also included the statement, in describing the citation to Jaffe, that it is well-known that table lookups of pre-computed values can increase processing speed (see page 10 of the previous Office action). Official notice is now explicitly taken of this fact below, and the explanation of the rejection has been clarified accordingly.

Applicant additionally reasserts the opinion that Jaffe has been misinterpreted as applied in the present application (see page 9 of the present response). Applicant does acknowledge that Jaffe discloses the use of a constant Hamming weight representation of data (page 9 of the present response, citing Jaffe, column 4, lines 56-67). However, Applicant further states that Jaffe "does not show 'each of two different data in the constant Hamming weight are before and after the predetermined operation, each other'" (page 10 of the present response, emphasis in original). The Examiner fails to appreciate this argument; it does not appear to make grammatical sense, nor is it apparent from where Applicant is drawing the quoted portions.

Applicant further argues that "Jaffe does not teach that two different data have the constant Hamming weight as each other [sic] before and after the predetermined operation" (page 11 of the present response, emphasis removed). However, Jaffe discloses or at least suggests that all data in a system would be represented using the disclosed constant Hamming weight representation (see Jaffe, column 2, lines 56-60, as previously cited, the "basic representation of data" is changed). Therefore, any pieces of data (with the same length) will have the same Hamming weight before and after any processing done using such a constant Hamming weight representation (see also Jaffe, column 4, line 55-column 5, line 30).

Similarly, Applicant alleges that "if the first and second disturbance data of Applicant admitted prior art are given 'a constant Hamming weight representation' according to Jaffe, the second disturbance data computed by using the operation f (OP1) on the first disturbance data of [the admitted prior art] cannot guarantee its Hamming weight not to become 0 or 8" (page 11 of the present response). However, Applicant has not provided any evidence in support of this allegation, even though Jaffe explicitly describes the representations as always having constant Hamming weight (Jaffe, column 4, line 55-column 5, line 30; column 2, lines 56-60, as previously cited) in order to minimize the information leaked from cryptographic systems by power consumption fluctuations (see Jaffe, column 2, lines 44-48). Jaffe discloses that all the data in the system, no matter whether it is before or after some particular processing performed, has a constant Hamming weight (column 2, lines 56-60) and therefore this does ensure that the Hamming weight of an 8-bit word would not go to 0 or 8, but would

stay constant (for example, considering the examples at Jaffe, column 5, lines 9-15, the representations of all but the last example would give a constant Hamming weight of 4 for eight bits, whereas the last example would give a constant Hamming weight of 2 for eight bits; none of these go to 0 or 8). There is no indication that the term "constant" as used by Jaffe should be given anything other than its ordinary meaning, and therefore, regardless of whatever processing may be done on the data, its Hamming weight would remain constant (Jaffe, column 2, lines 56-60; column 4, line 55-column 5, line 30; see also column 5, line 31-column 6, line 36, where a fixed number of transitions can also be used in combination with the constant Hamming weight representations to further minimize leakage of information).

Finally, Applicant alleges that Jaffe's use of a constant Hamming weight representation "does not lead to the processed data D2 of the present invention" and that using the process of transforming data using disturbance data, processing the transformed data, and un-transforming the processed data using the processed disturbance data would not be produced (see pages 11-12 of the present response). However, Applicant provides no evidence or explanation in support of this allegation. Applicant asserts that application of Jaffe's constant Hamming weight representation to the first and second disturbance data would not result in them having the same constant Hamming weight "both before and after the predetermined operation" (page 12 of the present response). However, again, Applicant provides no evidence or explanation in support of this assertion, nor is it apparent to which "predetermined operation" the above portion is intended to refer. Further, again, this appears to contradict Jaffe's

explicit disclosure of the use of constant Hamming weight representations (see Jaffe, column 2, lines 56-60, as previously cited).

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Specification

3. The objection to the specification for failure to provide proper antecedent basis for the claimed subject matter is withdrawn in light of Applicant's statements pointing out where support for the limitations at issue is to be found in the specification (page 5 of the present response).

Claim Rejections - 35 USC § 112

4. The rejection of Claims 1 and 28 under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement is withdrawn in light of Applicant's statements pointing out where support for the limitations at issue is to be found in the specification (page 5 of the present response, citing page 35, line 10-page 37, line 13, of the specification, where the stored data "usable as the … disturbance data" is considered to provide support for the claimed stored "candidates"). The rejection of Claim 3 is moot in light of the cancellation thereof.

5. The rejection of Claims 1 and 28 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn because not all issues have been addressed and/or the amendments raise new issues, as detailed below. The rejection of Claim 3 is moot in light of the cancellation thereof.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1 and 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "said disturbance data" in lines 6-7. There does not appear to be clear antecedent basis for this limitation in the claim. The table of candidates of disturbance data appears to refer to multiple items of disturbance data (lines 5-6) and therefore it is unclear to which disturbance data the limitation is intended to refer. This renders the claim indefinite.

Claim 28 recites "said disturbance data XI of said candidate pairs" in line 6. The claim also recites multiple candidate pairs of disturbance data XI and XO in lines 5-6, and it is not clear to which of these multiple items of disturbance data XI is intended to refer. The wording of the phrase is also generally unclear as to whether the disturbance data XI is singular or plural, and therefore it is not clear if the same data XI is used for each candidate pair or if different data XI is present in each of the pairs. The claim further recites "selecting said pair of disturbance data XI and XO" in line 11. It is not

clear to which of the multiple candidate pairs recited in lines 5-6 this is intended to refer. This renders the claim indefinite.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a selector for selecting disturbance data; disturbance data processing means performing predetermined processing on the selected disturbance data to generate processed disturbance data; a data transform means transforming input data by using the selected disturbance data to generate transformed data; a transformed data processing means for performing predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for performing inverse transformation processing on the processed transformed data using the processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly

disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order to minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

Although Jaffe and the admitted prior art generally disclose selection of disturbance data (page 21, lines 1-12 of the present specification, where disturbance data is used and therefore inherently selected to be used prior to its use) and the general use of look-up tables (Jaffe, column 15, line 61-column 16, line 14), neither Jaffe nor the admitted prior art explicitly discloses selecting disturbance data from a table of candidates of disturbance data. However, Official notice is taken that it is well-known that table lookups of pre-computed values can increase processing speed during critical operations by shifting the processing load to earlier in the process (or to earlier processes such as initialization). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the apparatus of the prior art to include a table of pre-calculated candidates of disturbance data that maintain a constant Hamming weight (as taught by Jaffe as detailed above) in order to realize the well-known predictable result of increased processing speed.

In reference to Claim 28, Applicant admits as prior art an apparatus including a selector for selecting disturbance data and that processed disturbance data is obtained by performing predetermined processing on the selected disturbance data; a data transform means transforming input data by using the selected disturbance data to generate transformed data; a transformed data processing means for performing predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for performing inverse transformation processing on the processed transformed data using the processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order to minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

Although Jaffe and the admitted prior art generally disclose selection of disturbance data (page 21, lines 1-12 of the present specification, where disturbance data is used and therefore inherently selected to be used prior to its use) and the

general use of look-up tables (Jaffe, column 15, line 61-column 16, line 14), neither Jaffe nor the admitted prior art explicitly discloses selecting disturbance data from a table of candidates of disturbance data. However, Official notice is taken that it is well-known that table lookups of pre-computed values can increase processing speed during critical operations by shifting the processing load to earlier in the process (or to earlier processes such as initialization). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the apparatus of the prior art to include a table of pre-calculated candidates of disturbance data that maintain a constant Hamming weight (as taught by Jaffe as detailed above) in order to realize the well-known predictable result of increased processing speed.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2437